東京理科大学
TOKYO UNIVERSITY OF SCIENCE

Video Tampering Detection Using Machine Learning

Hiroki Ueda[1], Hyunho Kang, Keiichi Iwamura
[1]Department of Electrical Engineering
Tokyo University of Science
Tokyo, JAPAN

Contents

1 . Background

Recently, security cameras have been installed in various places.

1 . Background

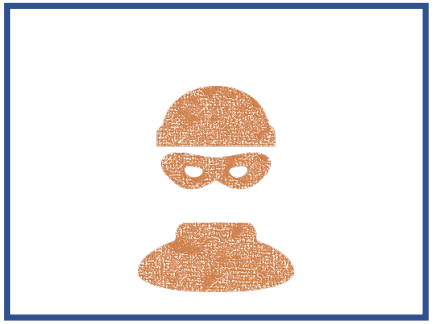
Security Camera

Smartphone

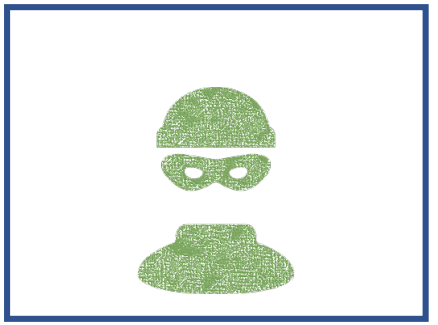
Drive Recorder

Video

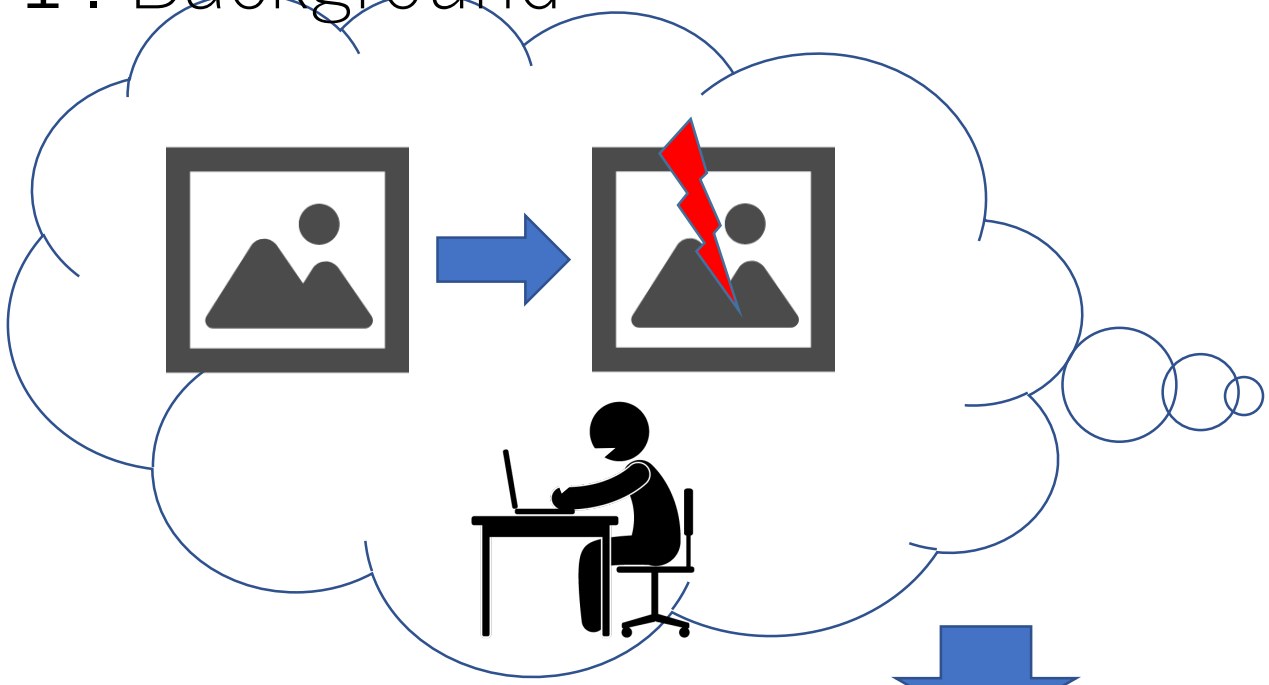
Image



Tampering

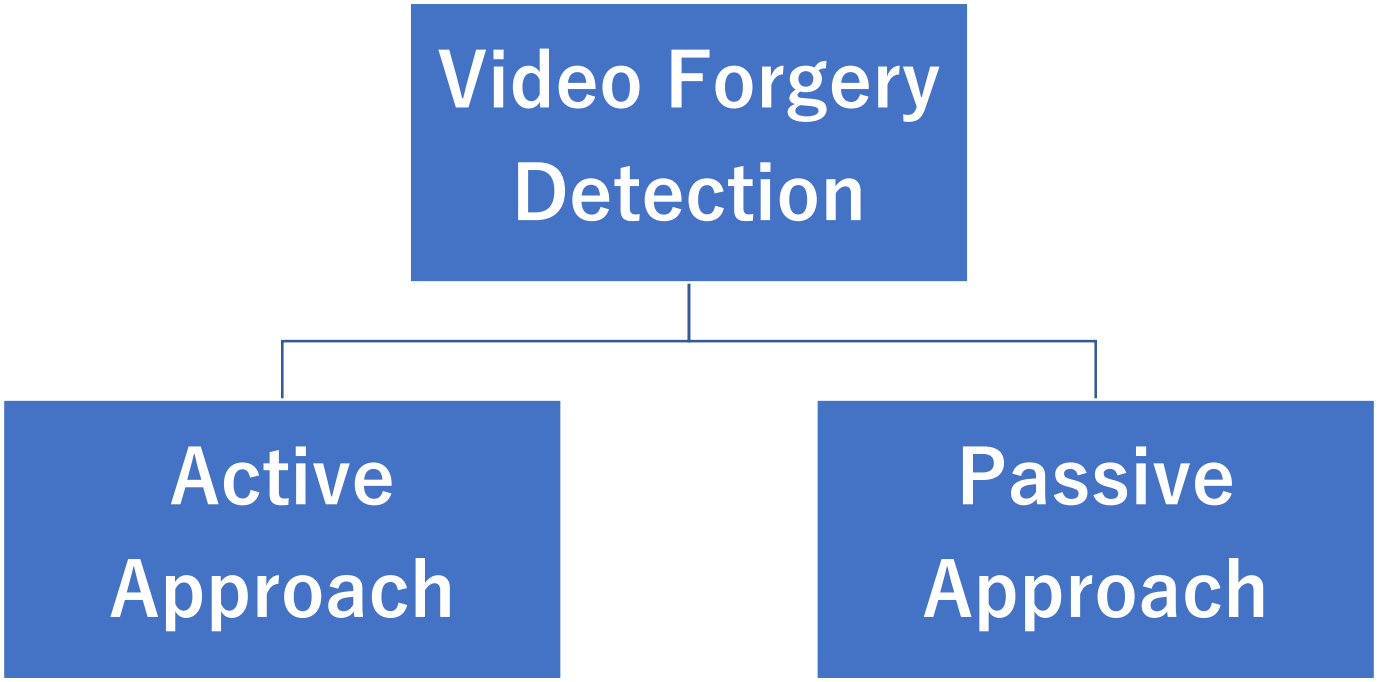


1 . Background

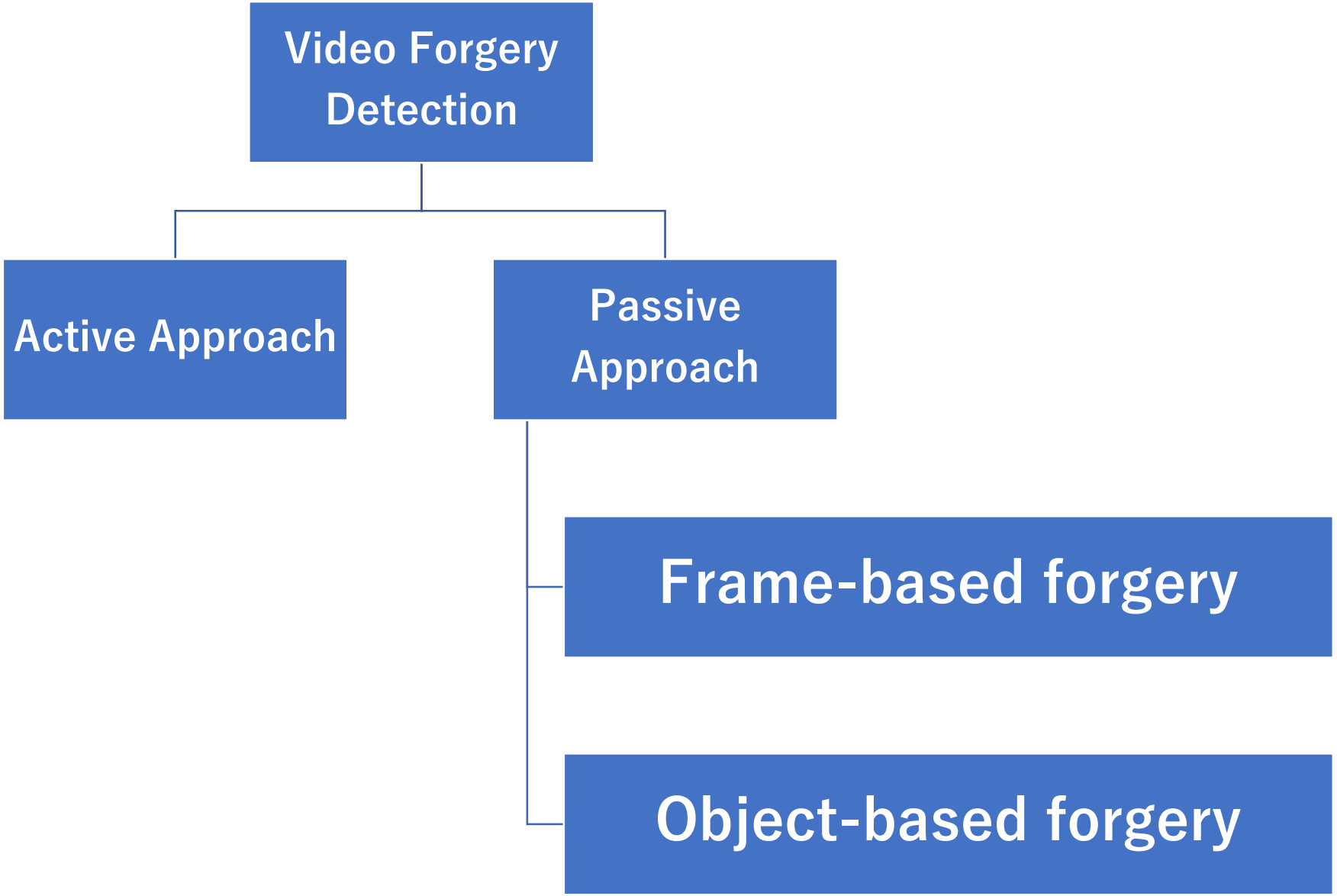


The video or image from a security camera can be used to provide legal evidence.

1 . Background



1. Background



◇ Process of Verification

① Preparation of dataset

② Preprocessing of dataset

③ Separation of dataset for training and verification

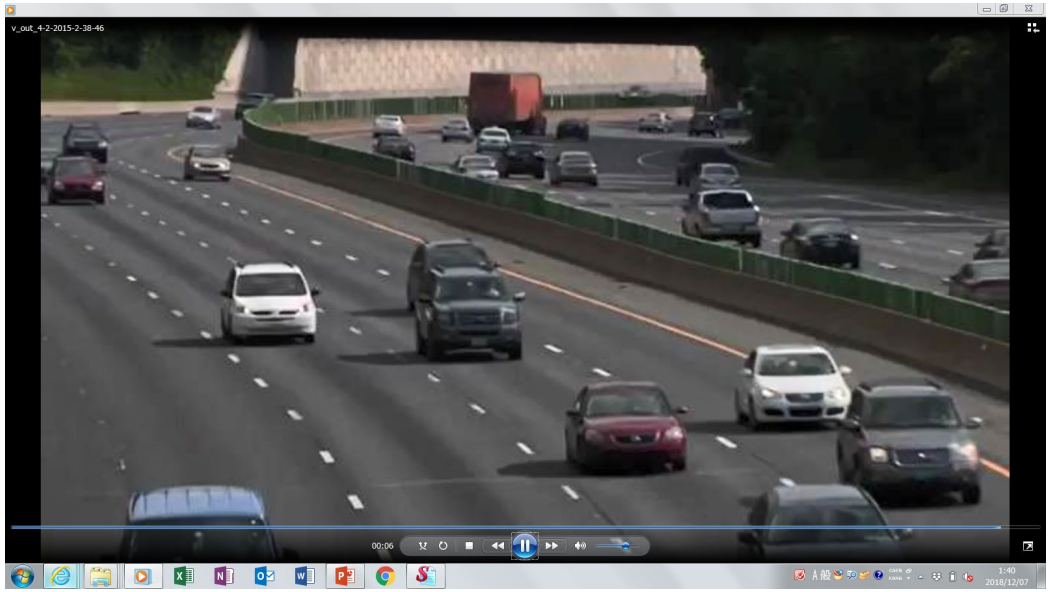
④ Generation of classifier that identify whether there is any manipulation

⑤ Verification of forgery using dataset for verification

2.1. Conventional Method –Preparation of Dataset-

- Tampered Video Dataset

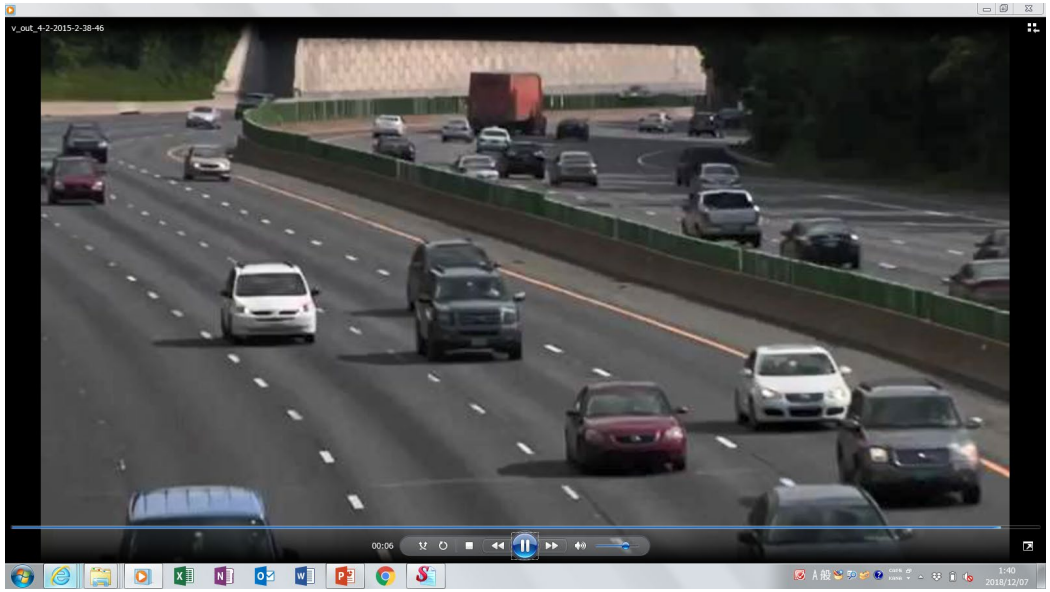
- One original video
- A video with eight patterns of tampering added to it
- Eight patterns of tampering added are as follows:
  Multiple / Rotation / No transformation / RGB /
  Shearing / Scaling / Brightness / Flipping



Released by the CVIP GROUP

2.1. Conventional Method –Preparation of Dataset-

- Tampered Video Dataset



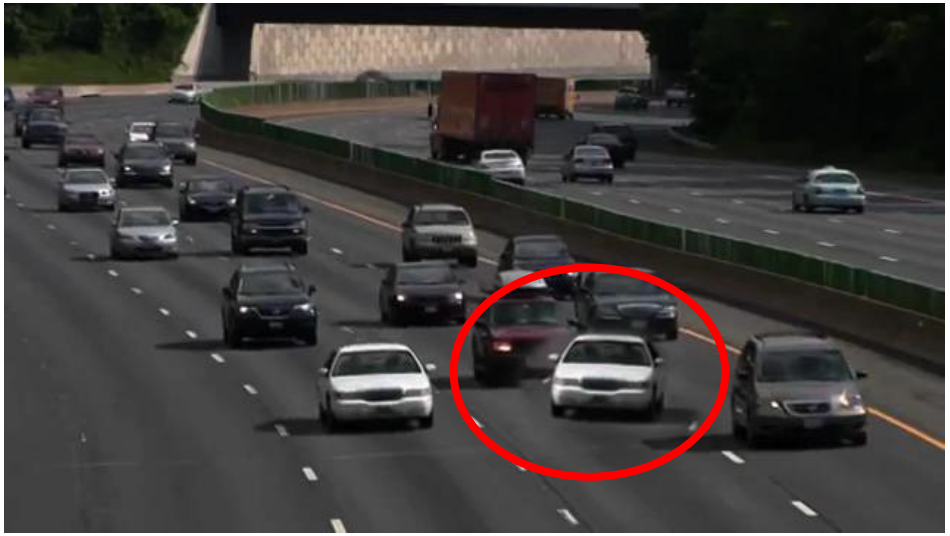
- Dimensions: 640×360
- Length: 5 [s] ～ 10 [s]
- Framerate: 25 [fps]

Ex.)

2.1. Conventional Method –Preparation of Dataset-

No Tampering

Tampering



◇ Process of Verification

① Preparation of dataset

② Preprocessing of dataset

③ Separation of dataset for training and verification

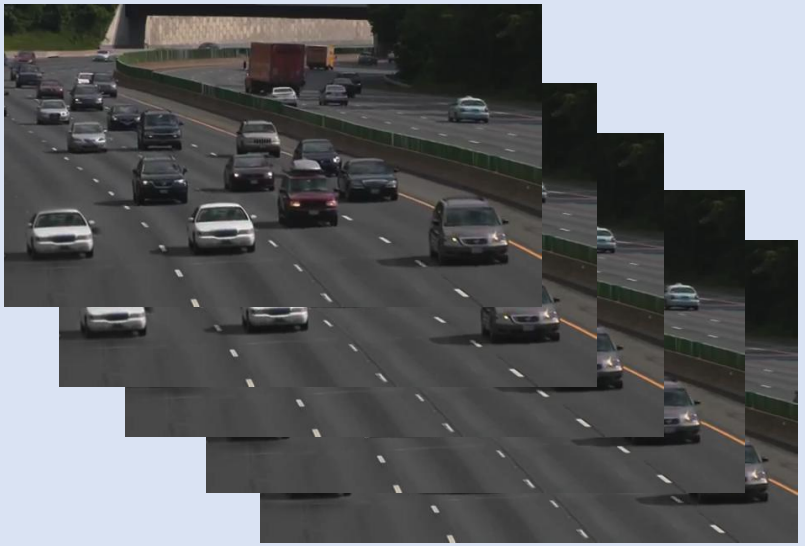
④ Generation of classifier that identify whether there is any manipulation

⑤ Verification of forgery using dataset for verification

2.2. Conventional Method –Preprocessing of Dataset-

Dataset

640×360 , 25 f/s



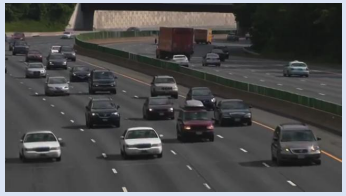
The video is divided into frames and stored as images (jpeg format)

2.2. Conventional Method –Preprocessing of Dataset-

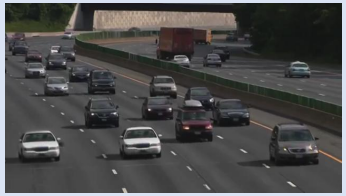
Dataset

Divided

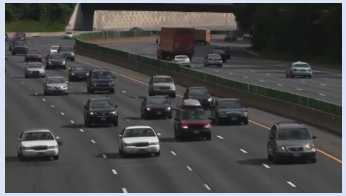
①



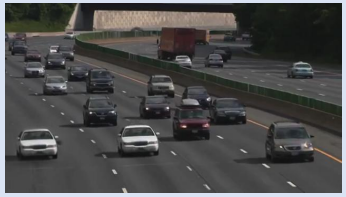
②



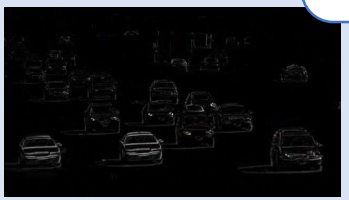
③



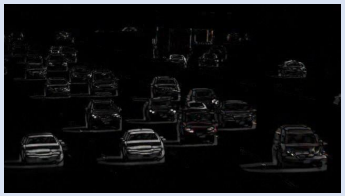
④



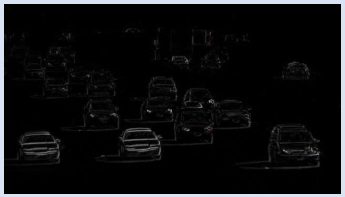
⑤



← A



← B

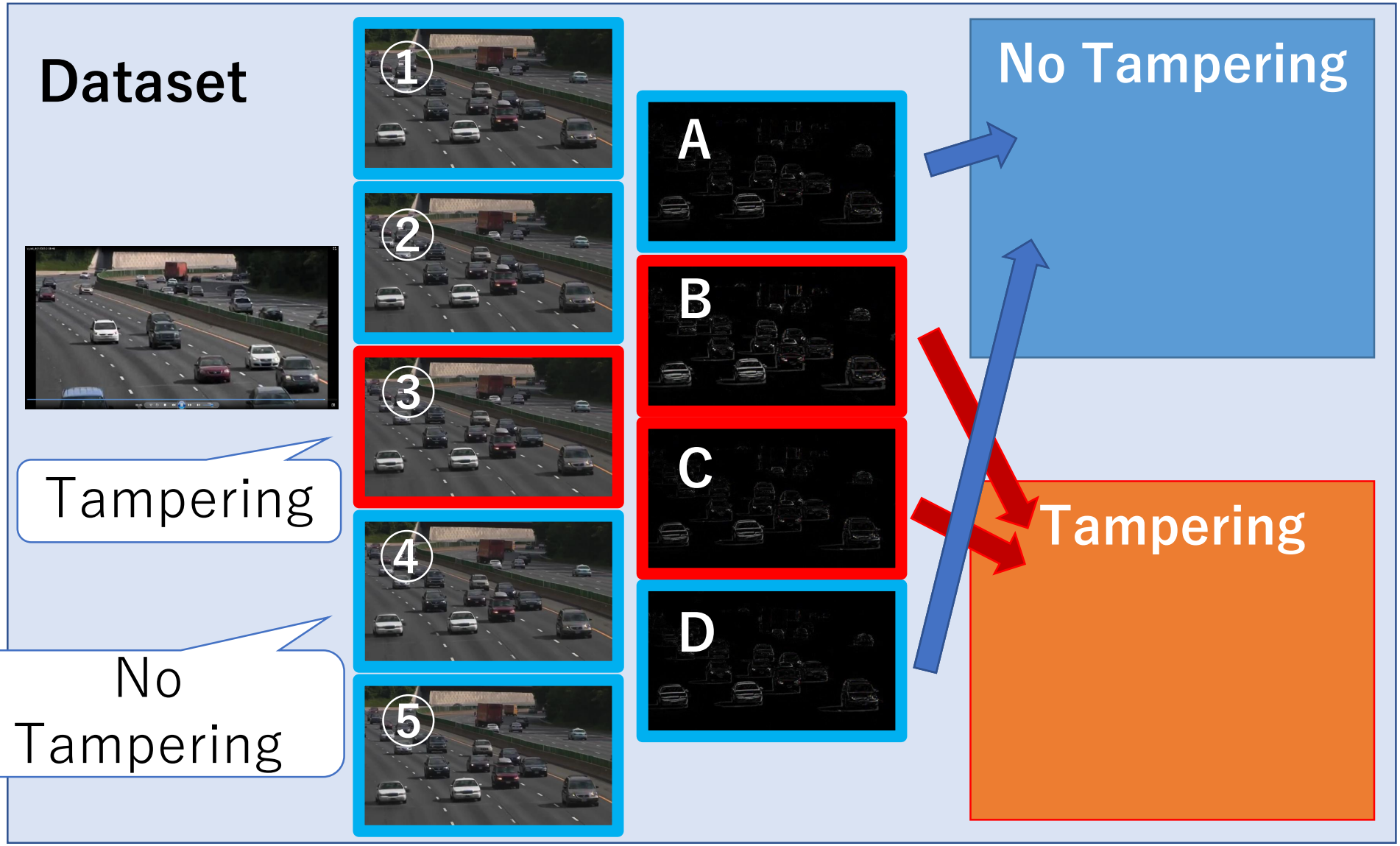


← C

← D

Variation Frame

2.2. Conventional Method –Preprocessing of Dataset-



2.2. Conventional Method –Preprocessing of Dataset-

Dataset

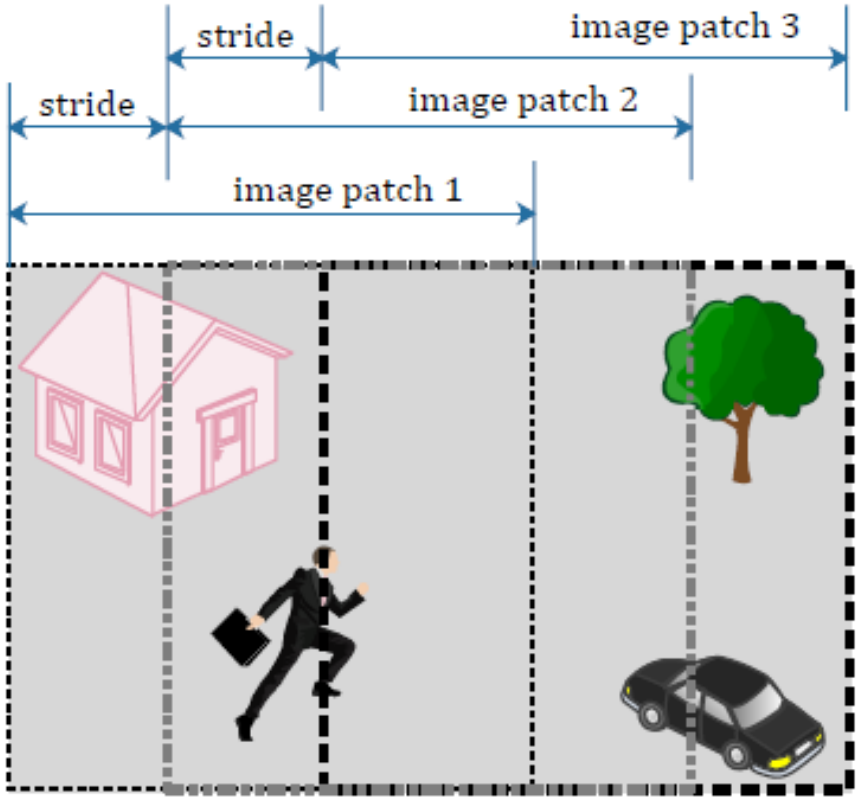
	Multiple	No transformation	Shearing	Brightness	Rotation	RGB	Scaling	Flipping
No Tampering	151	141	141	140	141	141	158	141
Tampering	20	30	30	31	30	30	13	30

(Number of frames)

Acquisition of Patch Image

Tampering … Positive
No Tampering … Negative

Deep Learning for Detection of Object-Based Forgery in Advanced Video
Ye Yao , Yunqing Shi , Shaowei Weng , Bo Guan
Symmetry 2018

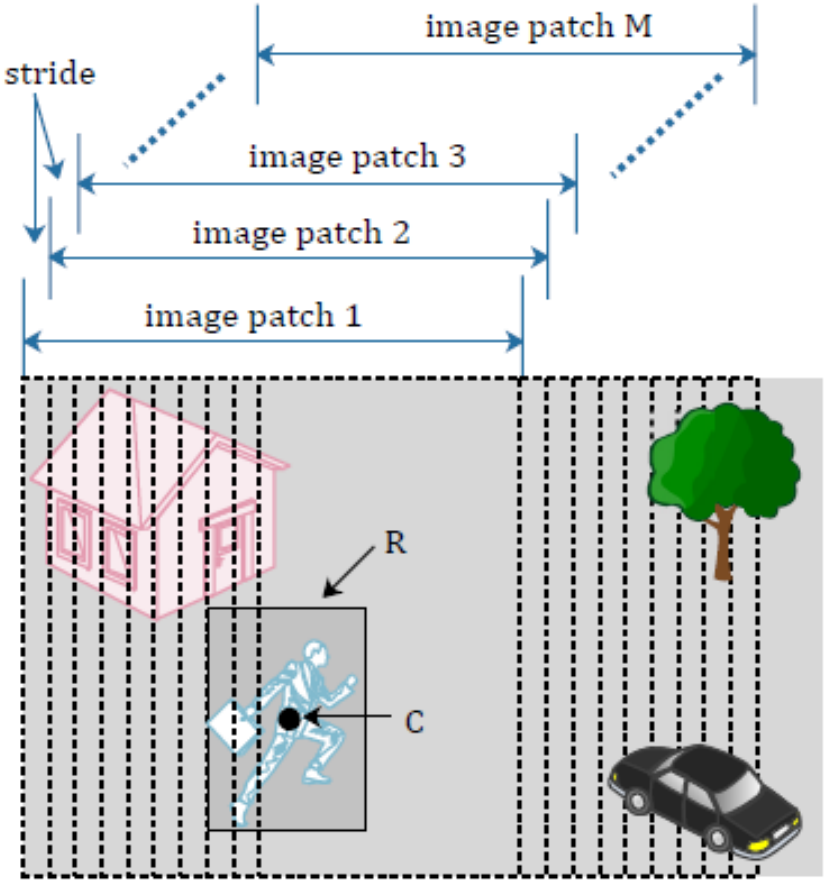


(a)

In a frame that has not been tampered, the variation frame is trimmed into three sheets comprising of left, center, and right blocks.

Acquisition of Patch Image

Tampering … Positive
No Tampering … Negative



(b)

In the tampered frame, the tampered portion is placed as centrally as possible, and split into 10 sheets, while being shifted by 1 to 3 pixels.

2.3. Conventional Method -Acquisition of Patch Image-

Dataset

		Trimming	Multiple	No transformation	Shearing	Brightness	Rotation	RGB	Scaling	Flipping
No Tampering	Before		151	141	141	140	141	141	158	141
	After		453	423	423	420	423	423	473	423
Tampering	Before		20	30	30	31	30	30	13	30
	After		200	300	300	310	300	300	131	300

"No Tampering" : "Tampering" ⇒ 141 : 30 = **4.7** : 1

After trimming ⇒ 423 : 300 = **1.4** : 1

◇ Process of Verification

① Preparation of dataset

② Preprocessing of dataset

③ Separation of dataset for training and verification

④ Generation of classifier that identify whether there is any manipulation

⑤ Verification of forgery using dataset for verification

◇ Process of Verification

① Preparation of dataset

② Preprocessing of dataset

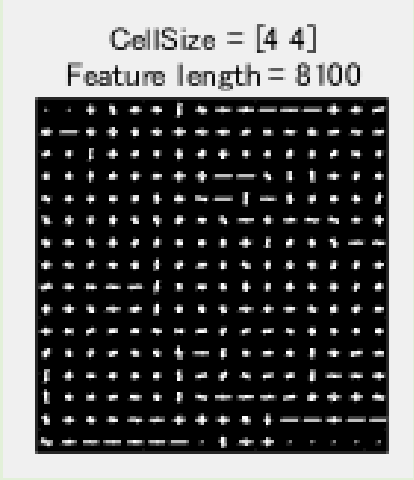
③ Separation of dataset for training and verification

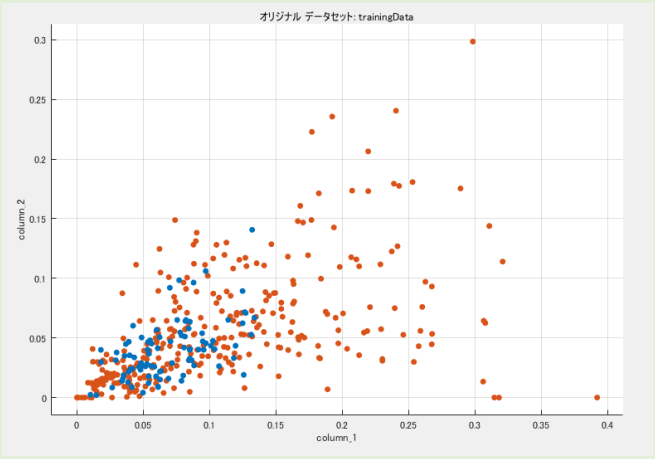
④ Generation of classifier that identify whether there is any manipulation

⑤ Verification of forgery using dataset for verification

2.4. Conventional Method –Workflow of Machine Learning-

Feature Extraction and Machine Learning



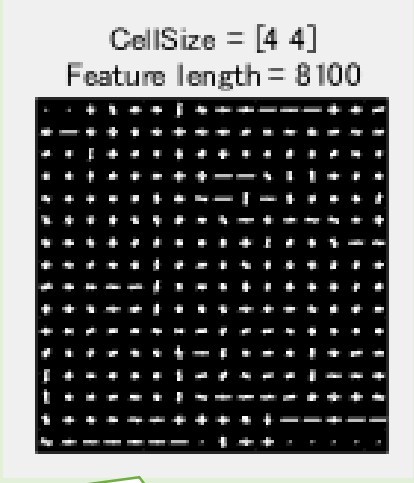


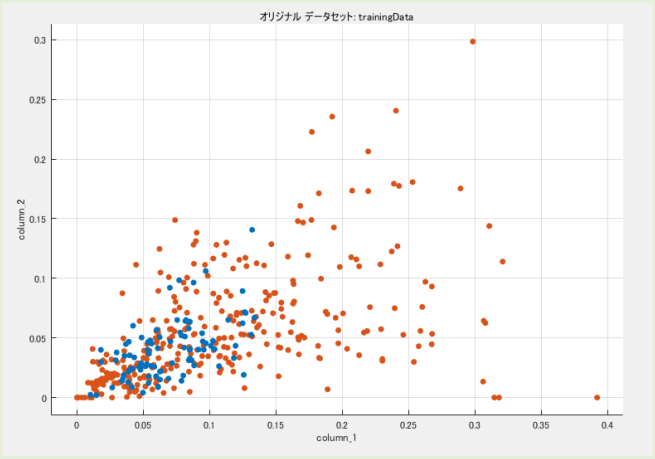
Trimmed Frame

※assigned with labels of “no tampering” and “tampering”

2.4. Conventional Method –Workflow of Machine Learning-

Feature Extraction and Machine Learning



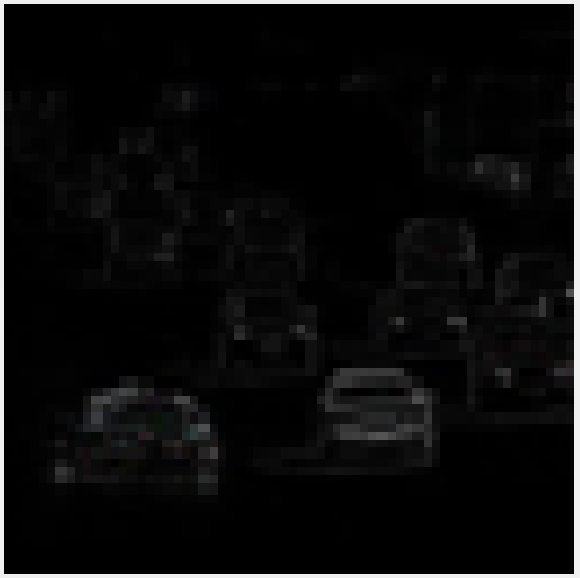


Feature Extraction

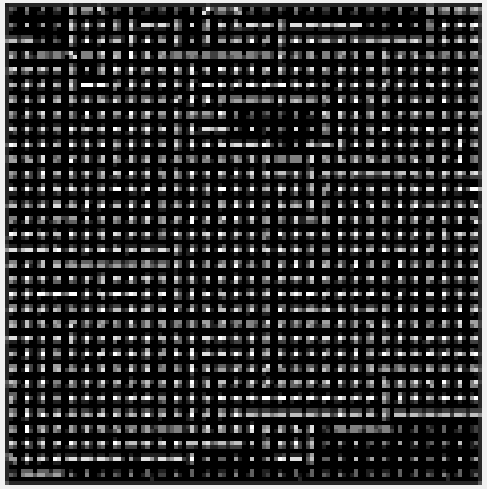
Histograms of Oriented Gradients

◇ Feature Extraction

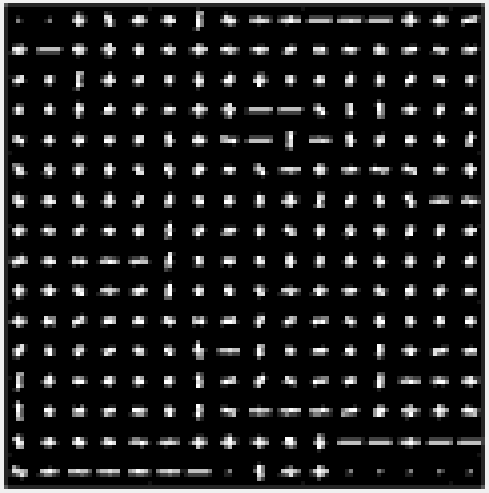
HOG(Histograms of Oriented Gradients)



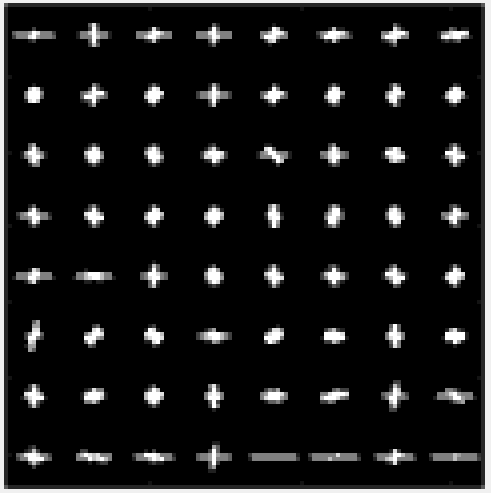
CellSize = [2 2]
Feature length = 34596



CellSize = [4 4]
Feature length = 8100

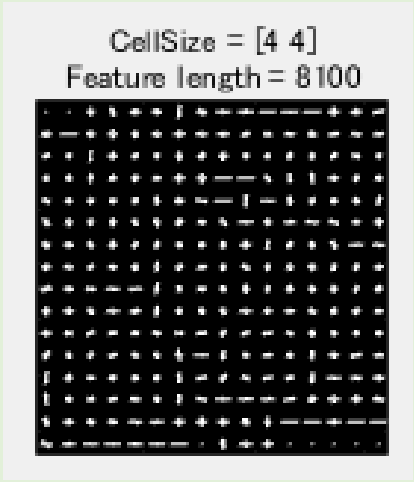


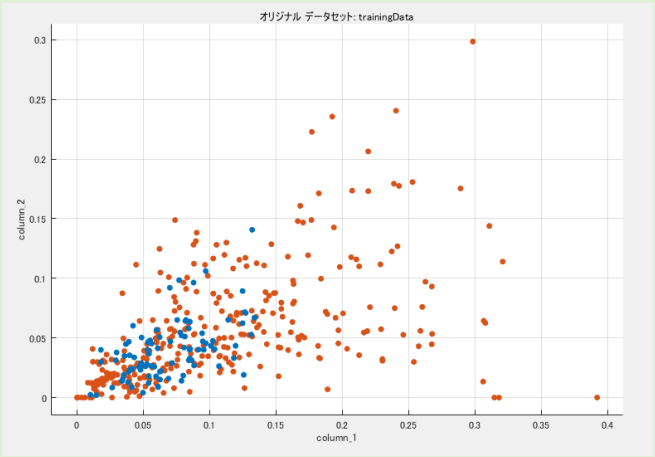
CellSize = [8 8]
Feature length = 1764



2.4. Conventional Method –Workflow of Machine Learning-

Machine Learning

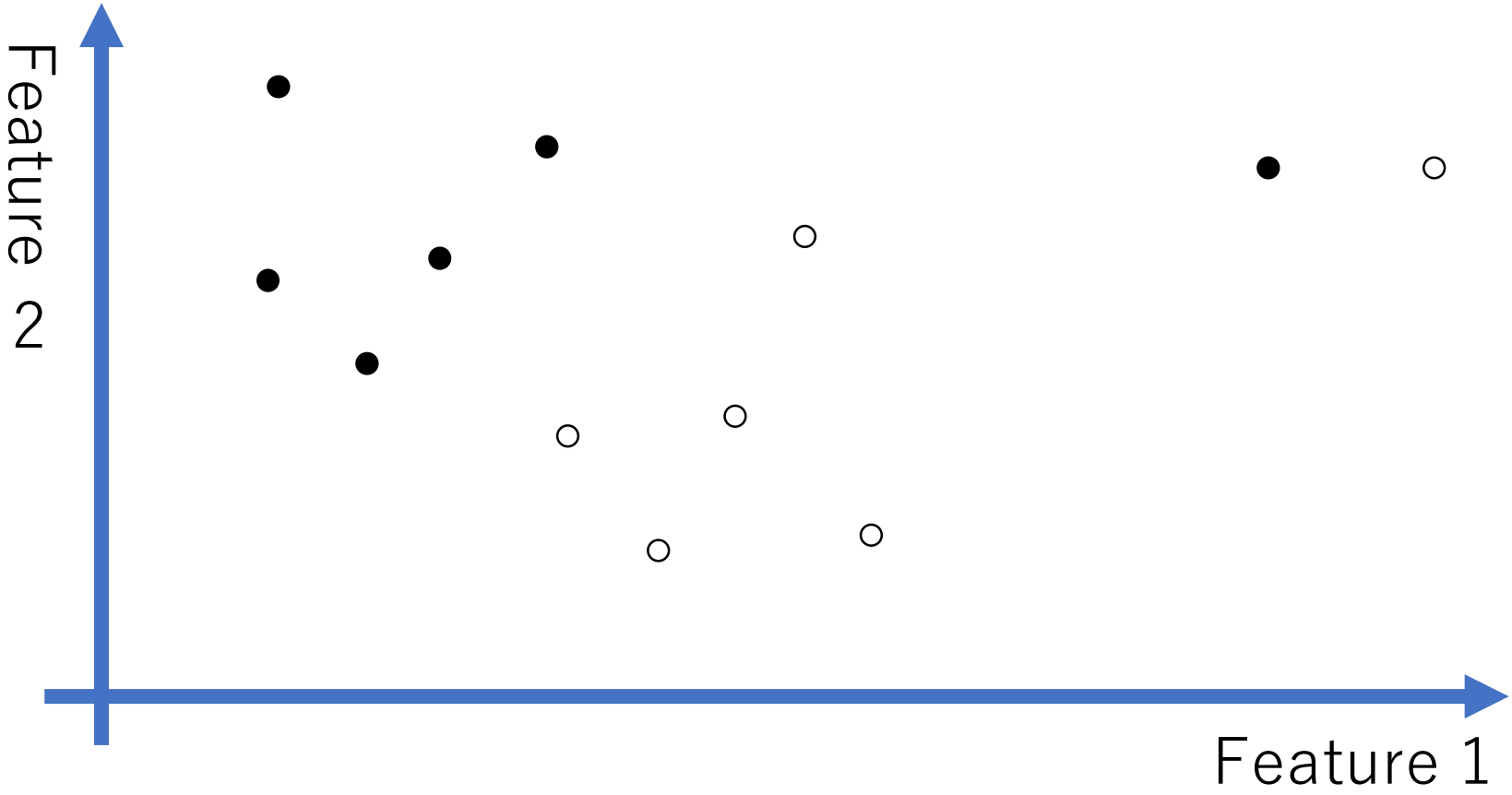




Generation of classifier that return whether there is manipulation using machine learning ⇒ SVM

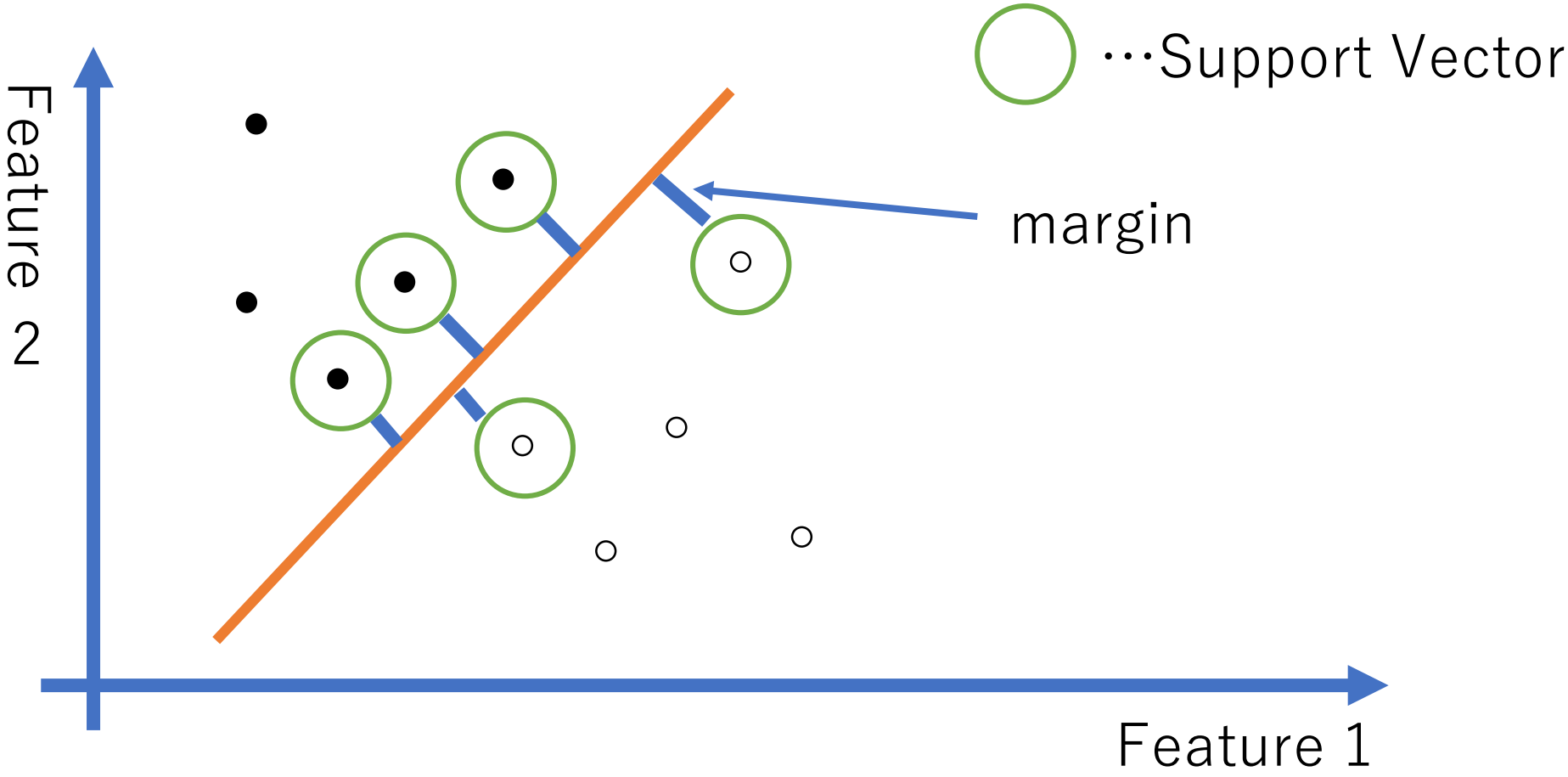
◇ Support Vector Machine (SVM)

Supervised Learning
= Using labeled training data



◇ Support Vector Machine (SVM)

Supervised Learning
= Using labeled training data



□ Changes Made Over the Conventional Method

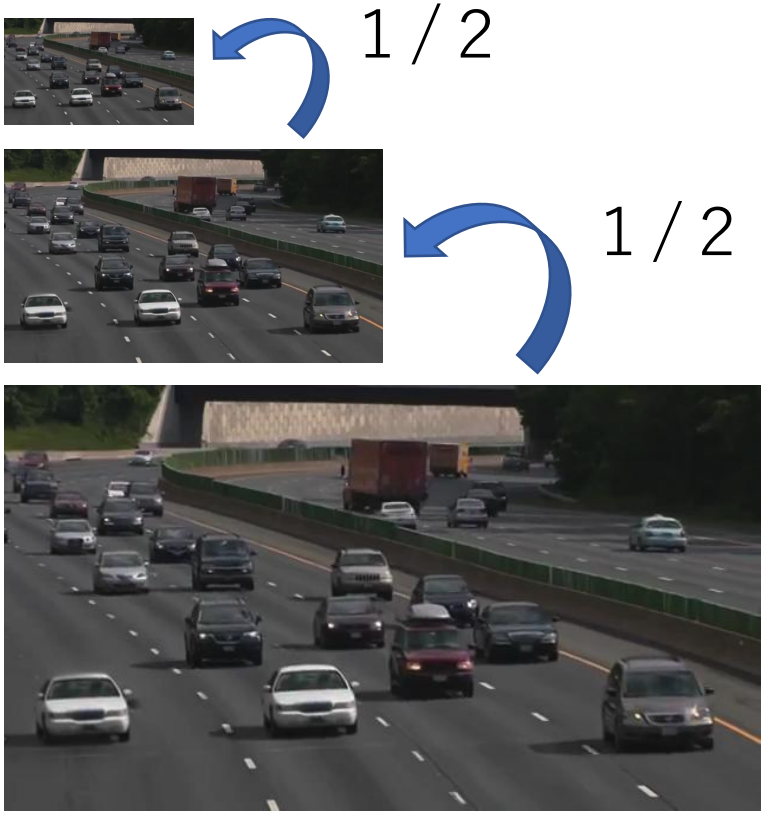
- Improvement in the accuracy of detection
  ⇒ **By using the high frequency feature of consecutive frames**

- Because the dataset for the verification and training have the same origin, it is not practical for verification.
  ⇒ Origin for each dataset is taken separately

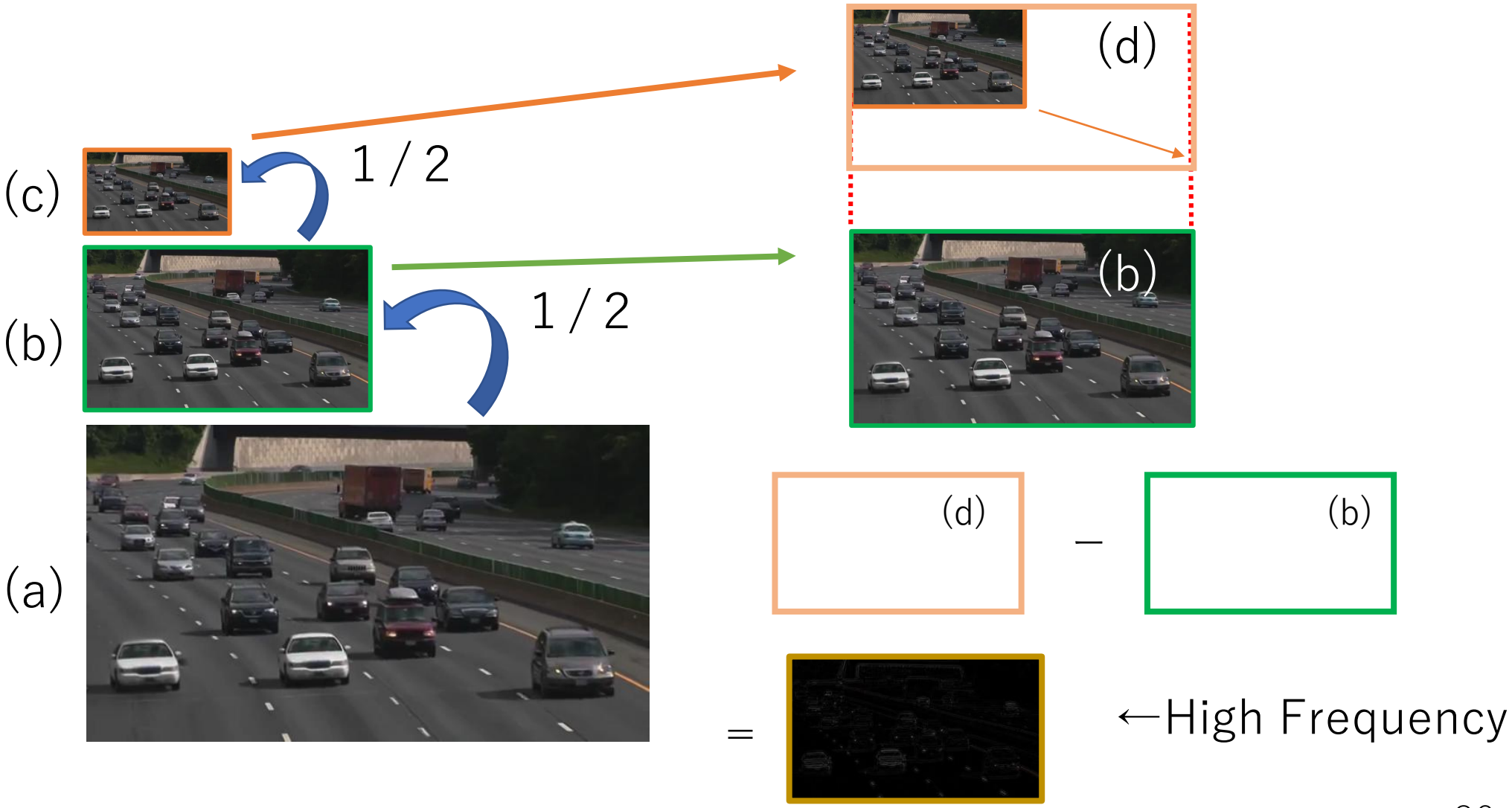
- Addition of evaluation parameters

3.1. Proposed Method –Improvement of Feature Extraction-

We used the **high frequency** feature of consecutive frames.
⇒ Implementation of **Gaussian Pyramid**



3.1. Proposed method –Improvement of Feature Extraction-



◇ Process of Verification

① Preparation of dataset

② Preprocessing of dataset

③ Separation of dataset for training and verification

④ Generation of classifier that identify whether there is any manipulation

⑤ Verification of forgery using dataset for verification

□ Changes From the Conventional Method

- Improvement detection accuracy
  ⇒ the feature of high frequency of consecutive frames

- Because dataset for the verification has the same origin of dataset for the training, it is not practical verification.
  ⇒ Each origin separately

- Addition evaluation parameters

Evaluation Parameters

	Tampering	No Tampering
Positive	TP = True Positive	FP =False Positive
Negative	FN =False Negative	TN =True Negative

number of frames

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

Evaluation Parameters

$$F1\ Score$$

$$= \frac{1}{\frac{1}{2}\left(\frac{1}{Precision} + \frac{1}{Recall}\right)}$$

$$= 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

F1 Score is the harmonic mean of Precision and Recall.

3.2. Proposed method –Result of Verification-

	Conventional method	Proposed method 1	Proposed method 2
Accuracy	**80.6%**	**82.6%**	**87.6%**
Precision	100.0%	100.0%	100.0%
Recall	53.3%	57.8%	63.0%
F1 Score	**69.3%**	**73.3%**	**77.3%**

3.2. Proposed method –Result of Verification-

	Multiple	No Trans.	Shearing	Brightness	Rotation	RGB	Scaling	Flipping
Accuracy	**88.78%**	**87.56%**	**88.94%**	**80.82%**	**88.94%**	**85.25%**	**94.54%**	**80.18%**
Precision	100.00%	100.00%	100.00%	100.00%	100.00%	95.31%	100.00%	100.00%
Recall	63.33%	70.00%	73.33%	54.84%	73.33%	67.78%	76.19%	52.22%

- ✓ In most tampering patterns, False Positive (FP) = 0
- ✓ Recall ⇒ Uneven
  - ⇒ Tampering with a small change in luminance was detected with a low recall value.

Conclusions

- ☑ High Frequency feature in an image was proven to be effective as a parameter for forgery detection.
- ☑ With the improvement of the verification method, our proposed method is practical for forgery detection.